AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A computer controlled method in a provisioning device in a networked computer system comprising an execution mechanism configured to execute the method, the method comprising:

establishing communication between the provisioning device and the network device over a preferred channel, wherein the preferred channel is a bidirectional, location-limited channel which has a demonstrative identification property and an authenticity property;

pre-authenticating said network device, wherein pre-authenticating said network device involves:

exchanging key commitment information ~~over said preferred channel~~ between said provisioning device and said network device over said bidirectional preferred channel~~to pre-authenticate said network device~~;

exchanging keys between said provisioning device and said network device over a bidirectional channel that does not have to be the preferred channel; and

verifying the received keys using the received key commitment information on both the said provisioning device and said network device;

providing provisioning information to said network device over said bidirectional preferred channel, wherein the provisioning information comprises:

a first set of provisioning information which is used exclusively to establish secure and authenticated communication between the provisioning device and the said network device using a second channel, wherein the second channel need not be location-limited; and

other provisioning information;

whereby said network device can automatically configure itself for secure communication over a network responsive to said first and other provisioning information, wherein the secure communication can be over the second channel.

2. (Original) The computer controlled method of claim 1, wherein said provisioning information comprises network configuration information.

3. (Original) The computer controlled method of claim 1, further comprising

receiving a public key from said network device;

verifying said public key with said key commitment information; and

automatically provisioning said network device with a credential authorized by a credential issuing authority.

4. (Original) The computer controlled method of claim 3, further comprising establishing proof that said network device is in possession of a private key corresponding to said public key.

5. (Original) The computer controlled method of claim 3, wherein said credential issuing authority is a certification authority and said credential is a public key certificate.

6. (Original) The computer controlled method of claim 3, wherein the step of automatically provisioning is responsive to authorization from a registration agent.

7-8 (Canceled).

9. (Original) The computer controlled method of claim 1, wherein the network is a wireless network, and wherein said provisioning device is a wireless access point.

10. (Original) The computer controlled method of claim 9, further comprising:

receiving a wireless communication;

determining whether said wireless communication originated from said network device or from a second network device that was not provisioned by said wireless access point; and

routing said wireless communication responsive to the step of determining.

11. (Original) The computer controlled method of claim 10, wherein the step of routing comprises:

choosing a selected channel from a secure channel and an insecure channel responsive to the step of determining; and

sending said wireless communication through said selected channel.

12. (Original) The computer controlled method of claim 1, wherein said provisioning device is in communication with a credential issuing authority.

13. (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method to provision a network device, the method comprising steps of:

establishing communication between the provisioning device and said network device over a preferred channel, wherein the preferred channel is a bidirectional, location-limited channel which has a demonstrative identification property and an authenticity property;

pre-authenticating said network device, wherein pre-authenticating said network device involves:

exchanging key commitment information ~~over said preferred channel~~ between said provisioning device and said network device over said bidirectional preferred~~to pre-authenticate said network device~~;

exchanging keys between said provisioning device and said network device over a bidirectional channel that does not have to be the preferred channel; and

verifying the received keys using the received key commitment information on both the said provisioning device and said network device;

providing provisioning information to said network device over said bidirectional preferred channel, wherein the provisioning information comprises:

a first set of provisioning information which is used exclusively to establish secure and authenticated communication between the provisioning device and the said network device using a second channel, wherein the second channel need not be location-limited; and

other provisioning information;

whereby said network device can automatically configure itself for secure communication over a network responsive to said first and other provisioning information, wherein the secure communication can be over the second channel.

14. (Original) The computer-readable storage medium of claim 13, further comprising

receiving a public key from said network device;

verifying said public key with said key commitment information; and

automatically provisioning said network device with a credential authorized by a credential issuing authority.

15. (Original) The computer-readable storage medium of claim 13, wherein the network is a wireless network, and wherein said provisioning device is a wireless access point.

16. (Currently amended) An apparatus for provisioning a network device comprising:

at least one port configured to establish a preferred channel;

a preferred communication mechanism configured to be able to establish communication with and said network device over said preferred channel, wherein the preferred channel is a bidirectional, location-limited channel which has a demonstrative identification property and an authenticity property;

a pre-authentication mechanism configured to be able to:

receive key commitment information over said preferred channel from said network device;

exchange keys between said provisioning device and said network device over a bidirectional channel that does not have to be the preferred channel; and verify the received keys using the received key commitment information on both said provisioning device and said network device;

a provisioning mechanism configured to provide provisioning information to said network device over said bidirectional preferred channel, wherein the provisioning information comprises:

a first set of provisioning information which is used exclusively to establish secure and authenticated communication between the provisioning device and the said network device using a second channel, wherein the second channel need not be location-limited ; and

other provisioning information;

whereby said network device can automatically configure itself for secure communication over a network responsive to said first and other provisioning information, wherein the secure communication can be over the second channel.

17. (Original) The apparatus of claim 16, wherein said provisioning information comprises network configuration information.

18. (Original) The apparatus of claim 16, further comprising

a key reception mechanism configured to receive a public key;

a key verification mechanism configured to verify said public key with said key commitment information; and

a credential provisioning mechanism configured to automatically provide a credential authorized by a credential issuing authority.

19. (Original) The apparatus of claim 18, further comprising a key exchange mechanism configured to be able to perform a key exchange protocol with said network device.

20. (Original) The apparatus of claim 18, wherein said credential issuing authority is a certification authority and said credential is a public key certificate.

21-22 (Canceled).

23. (Original) The apparatus of claim 22, further comprising:

a packet receiver mechanism configured to receive a wireless communication;

a determination mechanism configured to determine whether said wireless communication received by the packet receiver mechanism originated from said network device or from a second network device that was not provisioned by said wireless access point; and

a router mechanism configured to route said wireless communication responsive to the determination mechanism.

24. (Original) The apparatus of claim 23, wherein the router mechanism further comprises:

a channel selection mechanism configured to choose a selected channel from a secure channel and an insecure channel responsive to the determination mechanism; and

a transmission mechanism configured to send said wireless communication through said selected channel.

25. (Original) The apparatus of claim 16, further comprising a non-preferred communication mechanism that can be used to communicate with a credential issuing authority.

26-66. (Canceled)